CLAIMS:

What is claimed is:

1. A method in a node for managing authorized attempts to access the node, the method comprising:

receiving a packet from a source, wherein the packet includes a first key;

determining whether the first key matches a second key for the node;

dropping the packet without a response to the source if the first key does not match the second key;

storing information from the packet; and

sending the information to a selected recipient in response to a selected event.

2. The method of claim 1, wherein the selected event is a request from the recipient for the information.

3. The method of claim 1, wherein the selected event is an occurrence of a trap.

4. The method of claim 1, wherein the selected event is a periodic event.

5. The method of claim 1 further comprising:

incrementing a counter source if the first key does not match the second key.

6. The method of claim 1, wherein the selected event occurs when the counter exceeds a threshold value.

7. The method of claim 1, wherein the key is a partition key.

8. The method of claim 1, wherein the information includes at least one of a source local identifier, a destination local identifier, the key value, a global identifier address.

9. The method of claim 1, wherein the selected recipient is a subnet manager.

10. A method in a node for reporting access violations, the method comprising:

receiving a packet from a source, wherein the packet includes authentication information;

verifying the authentication information;

dropping the packet without a response to the source if authentication information is unverified;

storing information from the packet; and

sending the information to a selected recipient in response to a selected event.

11. The method of claim 10, wherein the information includes at least one of a source local identifier, a destination local identifier, the key value, a global identifier address.

12. A data processing system comprising:

a bus system;

a channel adapter unit connected to a system area

network fabric;

a memory connected to the bus system, wherein the memory includes as set of instructions; and

a processing unit connected to the bus system, wherein the processing unit executes the set of instructions to receive a packet from a source, wherein the packet includes a first key; determine whether the first key matches a second key for the node; drop the packet without a response to the source if the first key does not match the second key; store information from the packet; and send the information to a selected recipient in response to a selected event.

13. A node comprising:

receiving means for receiving a packet from a source, wherein the packet includes a first key;

determining means for determining whether the first key matches a second key for the node;

dropping means for dropping the packet without a response to the source if the first key does not match the second key;

storing means for storing information from the packet; and

sending means for sending the information to a selected recipient in response to a selected event.

14. The node of claim 13, wherein the selected event is a request from the recipient for the information.

15. The node of claim 13, wherein the selected event is an occurrence of a trap.

16. The node of claim 13, wherein the selected event is a periodic event.

17. The node of claim 13 further comprising:

incrementing means for incrementing a counter source if the first key does not match the second key.

18. The node of claim 13, wherein the selected event occurs when the counter exceeds a threshold value.

19. The node of claim 13, wherein the key is a partition key.

20. The node of claim 13, wherein the information includes at least one of a source local identifier, a destination local identifier, the key value, a global identifier address.

21. The node of claim 13, wherein the selected recipient is a subnet manager.

22. A node comprising:

receiving means for receiving a packet from a source, wherein the packet includes authentication information;

verifying means for verifying the authentication information;

dropping means for dropping the packet without a response to the source if authentication information is unverified;

storing means for storing information from the packet; and

sending means for sending the information to a selected recipient in response to a selected event.

23. The node of claim 22, wherein the information includes at least one of a source local identifier, a destination local identifier, the key value, a global identifier address.

24. A computer program product in a computer readable medium for use in a node for managing authorized attempts to access the node, the computer program product comprising:

first instructions for receiving a packet from a source, wherein the packet includes a first key;

second instructions for determining whether the first key matches a second key for the node;

third instructions for dropping the packet without a response to the source if the first key does not match the second key;

fourth instructions for storing information from the packet; and

fifth instructions for sending the information to a selected recipient in response to a selected event.

25. A computer program product in a computer readable medium for use in a node for reporting access violations, the computer program product comprising:

first instructions for receiving a packet from a source, wherein the packet includes authentication

information;

second instructions for verifying the authentication information;

third instructions for dropping the packet without a response to the source if authentication information is unverified;

fourth instructions for storing information from the packet; and

fifth instructions for sending the information to a selected recipient in response to a selected event.